The President’s Commission on Critical Infrastructure Protection

Critical Foundations

Thinking Differently

> *“Our responsibility is to build the world of tomorrow by embarking on a period of construction—one based on current realities but enduring American values and interests…”*
>
> *President William J. Clinton*
> *National Security Strategy*

Introduction

The United States is in the midst of a tremendous cultural change—a change that affects every aspect of our lives. The cyber dimension promotes accelerating reliance on our infrastructures and offers access to them from all over the world, blurring traditional boundaries and jurisdictions. National defense is not just about government anymore, and economic security is not just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between the private sector and the federal government.

The federal government has an important role to play in defense against cyber threats—collecting information about tools that can do harm, conducting research into defensive technologies, and sharing defensive techniques and best practices. Government also must lead and energize its own protection efforts, and engage the private sector by offering expertise to facilitate protection of privately owned infrastructures.

In the private sector, the defenses and responsibilities naturally encouraged and expected as prudent business practice for owners and operators of our infrastructures are the very same measures needed to protect against the cyber tools available to terrorists and other threats to national security.

Venues for Change

Terrorist bombings of US forces in Saudi Arabia, the World Trade Center in New York City, and the federal building in Oklahoma City remind us that the end of the Cold War has not eliminated threats of hostile action against the United States.

In recognition of comparable threats to our national infrastructures, President Clinton signed Executive Order 13010 on July 15, 1996, establishing the President’s Commission on Critical

Infrastructure Protection. The Commission was chartered to conduct a comprehensive review and recommend a national policy for protecting critical infrastructures and assuring their continued operation.

Our Process—Who We Are and What We Did

Composition and Operation of the Commission

This was an unusually large commission with broad representation from federal departments and agencies and from the private sector. An Advisory Committee of industry leaders appointed by the President provided the perspective of the infrastructure owners and operators. A Steering Committee, composed of the Commission's Chairman and four top government officials, oversaw the Commission's work on behalf of the Principals Committee, which included Cabinet Officers, heads of agencies, and senior White House staff members.

The Commission generally operated by consensus. Every recommendation was discussed at length with the full Commission and most were revised several times before final approval. No Commissioner agreed completely with all of the recommendations. Nevertheless, each accepted the final report as a reasonable and balanced recommendation to the President.

Sector Studies

The Commission divided its work into five "sectors" based on the common characteristics of the included industries. The sectors are:

1. Information and Communications
2. Banking and Finance
3. Energy, Including Electrical Power, Oil and Gas
4. Physical Distribution
5. Vital Human Services

The Commission characterized the sectors, studied their vulnerabilities, and looked for solutions.

We prepared comprehensive working papers for each of the five sectors providing specific recommendations. Other work contains the results of deliberations on issues that are not sector specific. Among them is a paper on *Research and Development Recommendations,* which outlines a comprehensive set of topics regarding the long term needs of infrastructure protection. The paper on *National Structures* contains our conclusions and recommendations about the functions and responsibilities for infrastructure assurance and the creation of new units in the federal government and the private sector, and some that are jointly staffed by government employees and representatives of the infrastructure owners and operators. The paper on *Shared Infrastructures: Shared Threats* is our collected analysis of the vulnerabilities and threats facing the critical infrastructures. We recognize the enormous significance of physical threats, but we have a significant amount of experience in dealing with them. It is the cyber threat that is new. Cyber issues dominate this analysis because networked information systems present fundamentally new security challenges.

Public Hearings and Outreach

We conducted extensive meetings with a range of professional and trade associations concerned with the infrastructures, private sector infrastructure users and providers, academia, different state and local government agencies, consumers, federal agencies, and numerous others. Of special interest were five public meetings in major cities.

We attended dozens of conferences and roundtables with a variety of groups, and we arranged two strategic simulations with participants drawn from across the infrastructures and from all levels of government. We encouraged questions and comments by anyone, and established a World Wide Web site to facilitate contact. Several meetings with Congressional Members and their staffs added a very useful perspective to our research.

Development of Our Critical Issues

During the preparation of the sector papers we identified several dozen issues for which recommendations might be appropriate. Each issue was described, relevant observations, findings, and conclusions were collected, and several alternative recommendations were prepared. The Commission then deliberated each issue and selected one of the alternative recommendations.

We Found

Increasing Dependence on Critical Infrastructures

The development of the computer and its astonishingly rapid improvements have ushered in the Information Age that affects almost all aspects of American commerce and society. Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers.

Increasing Vulnerabilities

Classical physical disruptions. A satchel of dynamite or a truckload of fertilizer and diesel fuel have been frequent terrorist tools. The explosion and the damage are so certain to draw attention that these kinds of attacks continue to be among the probable threats to our infrastructures.

New, cyber threats. Today, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people possess the skills necessary to consider such an attack. The wide adoption of public protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the resources needed to conduct a physical attack have not changed much recently, the resources necessary to conduct a cyber attack are now commonplace. A personal computer and a simple telephone connection to an Internet Service Provider anywhere in the world are enough to cause a great deal of harm.

System complexities and interdependencies. The energy and communications infrastructures especially are growing in complexity and operating closer to their designed capacity. This creates an increased possibility of cascading effects that begin with a rather minor and routine disturbance and end only after a large regional outage. Because of their technical complexity, some of these dependencies may be unrecognized until a major failure occurs.

A Wide Spectrum of Threats

Of the many people with the necessary skills and resources, some may have the motivation to cause substantial disruption in services or destruction of the equipment used to provide the service.

This list of the kinds of threats we considered shows the scope of activity with potentially adverse consequences for the infrastructures, and the diversity of people who might engage in that activity. It may not be possible to categorize the threat until the perpetrator is identified—for example, we may not be able to distinguish industrial espionage from national intelligence collection.

Natural events and accidents. Storm-driven wind and water regularly cause service outages, but the effects are well known, the providers are experienced in dealing with these situations, and the effects are limited in time and geography.

Accidental physical damage to facilities is known to cause a large fraction of system incidents. Common examples are fires and floods at central facilities and the ubiquitous backhoe that unintentionally severs pipes or cables.

Blunders, errors, and omissions. By most accounts, incompetent, inquisitive, or unintentional human actions (or omissions) cause a large fraction of the system incidents that are not explained by natural events and accidents. Since these usually only affect local areas, service is quickly restored; but there is potential for a nationally significant event.

Insiders. Normal operation demands that a large number of people have authorized access to the facilities or to the associated information and communications systems. If motivated by a perception of unfair treatment by management, or if suborned by an outsider, an "insider" could use authorized access for unauthorized disruptive purposes.

Recreational hackers. For an unknown number of people, gaining unauthorized electronic access to information and communication systems is a most fascinating and challenging game. Often they deliberately arrange for their activities to be noticed even while hiding their specific identities. While their motivations do not include actual disruption of service, the tools and techniques they perfect among their community are available to those with hostile intent.

Criminal activity. Some are interested in personal financial gain through manipulation of financial or credit accounts or stealing services. In contrast to some hackers, these criminals typically hope their activities will never be noticed, much less attributed to them. Organized crime groups may be interested in direct financial gain, or in covering their activity in other areas.

Industrial espionage. Some firms can find reasons to discover the proprietary activities of their competitors, by open means if possible or by criminal means if necessary. Often these are international activities conducted on a global scale.

Terrorism. A variety of groups around the world would like to influence US policy and are willing to use disruptive tactics if they think that will help.

National intelligence. Most, if not all, nations have at least some interest in discovering what would otherwise be secrets of other nations for a variety of economic, political, or military purposes.

Information warfare. Both physical and cyber attacks on our infrastructures could be part of a broad, orchestrated attempt to disrupt a major US military operation or a significant economic activity.

Lack of Awareness

We have observed that the general public seems unaware of the extent of the vulnerabilities in the services that we all take for granted, and that within government and among industry decision-makers, awareness is limited. Several have told us that there has not yet been a cause for concern sufficient to demand action.

We do acknowledge that this situation seems to be changing for the better. The public news media seem to be carrying relevant articles more frequently; attendance at conferences of security professionals is up; and vendors are actively introducing new security products.

The Commission believes that the actions recommended in this report will increase sensitivity to these problems and reduce our vulnerabilities at all levels.

No National Focus

Related to the lack of awareness is the need for a national focus or advocate for infrastructure protection. Following up on our report to the President, we need to build a framework of effective deterrence and prevention.

This is not simply the usual study group's lament that "no one is in charge." These infrastructures are so varied, and form such a large part of this nation's economic activity, that no one person or organization *can* be in charge. We do not need, and probably could not stand, the appointment of a *Director of Infrastructures.* We do need, and recommend, several more modest ways to create and maintain a national focus on the issues.

Protection of our infrastructures will not be accomplished by a big federal project. It will require continuous attention and incremental improvement for the foreseeable future.

We Concluded

Life on the information superhighway isn't much different from life on the streets; the good guys have to hustle to keep the bad guys from getting ahead.

Rules Change in Cyberspace—New Thinking is Required

It is not surprising that infrastructures have always been attractive targets for those who would do us harm. In the past we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports.

Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.

Formulas that carefully divide responsibility between foreign defense and domestic law enforcement no longer apply as clearly as they used to. "With the existing rules, you may have to solve the crime before you can decide who has the authority to investigate it."[*]

We Should Act Now to Protect our Future

The Commission has not discovered an imminent attack or a credible threat sufficient to warrant a sense of immediate national crisis. However, we are quite convinced that our vulnerabilities are increasing steadily while the costs associated with an effective attack continue to drop. What is more, the investments required to improve the situation are still relatively modest, but will rise if we procrastinate.

We should attend to our critical foundations before the storm arrives, not after: Waiting for disaster will prove as expensive as it is irresponsible.

Infrastructure Assurance is a Shared Responsibility

National security requires much more than military strength. Our world position, our ability to influence others, our standard of living, and our own self-image depend on economic prosperity and public confidence. Clear distinctions between foreign and domestic policy no longer serve our interests well.

At the same time, the effective operation of our military forces depends more and more on the continuous availability of infrastructures, especially communications and transportation, that are not dedicated to military use.

While no nation state is likely to attack our territory or our armed forces, we are inevitably the target of ill will and hostility from some quarters. Disruption of the services on which our eco-

[*] Senator Sam Nunn, remarks to the PCCIP Advisory Committee. Washington, DC, September 7, 1997.

nomy and well-being depend could have significant effects, and if repeated frequently could seriously harm public confidence. Because our military and private infrastructures are becoming less and less separate, because the threats are harder to differentiate as from local criminals or foreign powers, and because the techniques of protection, mitigation, and restoration are largely the same, we conclude that responsibility for infrastructure protection and assurance can no longer be delegated on the basis of who the attacker is or where the attack originates. Rather, the responsibility should be shared cooperatively among all of the players.

We Recommend

A Broad Program of Awareness and Education

Because of our finding that the public in general and many industry and government leaders are insufficiently aware of the vulnerabilities, we have recommended a broad and continuous program of awareness and education to cover all possible audiences. We include White House conferences, National Academy studies, presentations at industry associations and professional societies, development and promulgation of elementary and secondary curricula, and sponsorship of graduate studies and programs.

Infrastructure Protection through Industry Cooperation and Information Sharing

We believe the quickest and most effective way to achieve a much higher level of protection from cyber threats is to raise the level of existing protection through application of "best practices." We have accordingly recommended a sector-by-sector cooperation and information sharing strategy. In general, these sector structures should be partnerships among the owners and operators, and appropriate government agencies, which will identify and communicate best practices. We have especially asked the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to provide technical skills and expertise required to identify and evaluate vulnerabilities in the associated information networks and control systems.

One very effective practice is a quantitative risk management process, addressing physical attacks, cyber attacks that could corrupt essential information or deny service, the possibility of cascading effects, and new levels of interdependency.

The first focus of sector cooperation should be to share information and techniques related to risk management assessments. This should include development and deployment of ways to prevent attacks, mitigate damage, quickly recover services, and eventually reconstitute the infrastructure

We suggest consideration of these immediate actions prior to the completion of a formal risk assessment: (1) Isolate critical control systems from insecure networks by disconnection or adequate firewalls; (2) Adopt best practices for password control and protection, or install more modern authentication mechanisms; (3) Provide for individual accountability through protected action logs or the equivalent.

The sector cooperation and information sharing needed to improve risk assessments and to protect against probable attacks may naturally develop into sharing of information on current status. This would permit assessing whether one of the infrastructures is under a coordinated attack—physical, cyber, or combined. As this process develops, the national center for analysis of such information should be in place and ready to cooperate.

Reconsideration of Laws Related to Infrastructure Protection

Law has failed to keep pace with technology. Some laws capable of promoting assurance are not as clear or effective as they could be. Still others can operate in ways that may be unfriendly to security concerns. Sorting them all out will be a lengthy and massive undertaking, involving efforts at local, state, federal, and international levels. Recognizing the dynamic nature of legal reform, we attempted to lay a foundation through various studies, papers, and a legal authorities database that can aid eventual implementation of our recommendations and assist owners, operators, and government at all levels.

We also offered a number of preliminary legal recommendations intended to jump-start this process of reform. We identified existing laws that could help the government take the lead and serve as a model of standards and practices for the private sector. We identified other areas of law which, with careful attention, can enable infrastructure owners and operators to take precautions proportionate to the threat. We identified still other areas of law that should be molded to enable a greater degree of government-industry partnership in areas such as information sharing.

A Revised Program of Research and Development

The Commission believes that some of the basic technology needed to improve infrastructure protection already exists, but needs to be widely deployed. In other areas, additional research effort is needed.

At the same time the Commission recognizes that we are not now able to deploy several capabilities that we need. We have, therefore, recommended a program of research and development focused on those future capabilities. Among them are new capabilities for detection and identification of intrusion and improved simulation and modeling capability to understand the effects of interconnected and fully interdependent infrastructures.

A National Organization Structure

In order to be effective, recommendations must discuss not only what is to be done, but how it will get done and who will do it. We have recommended the following partnering organizations be established to be responsible for specific parts of our vision:

Sector Coordinators to provide the focus for industry cooperation and information sharing, and to represent the sector in matters of national cooperation and policy;

Lead Agencies, designated within the federal government, to serve as a conduit from the government into each sector and to facilitate the creation of sector coordinators, if needed;

National Infrastructure Assurance Council of industry CEOs, Cabinet Secretaries, and representatives of state and local government to provide policy advice and implementation commitment;

Information Sharing and Analysis Center to begin the step-by-step process of establishing a realistic understanding of what is going on in our infrastructures—of distinguishing actual attack from coincidental events;

Infrastructure Assurance Support Office to house the bulk of the national staff which is responsible for continuous management and follow-through of our recommendations; and

Office of National Infrastructure Assurance as the top-level policy making office connected closely to the National Security Council and the National Economic Council.

Conclusion

It is clear to us that infrastructure assurance must be a high priority for the nation in the Information Age. With escalating dependence on information and telecommunications, our infrastructures no longer enjoy the protection of oceans and military forces. They are vulnerable in new ways. We must protect them in new ways. And that is what we recommend in this report.

The public and private sectors share responsibility for infrastructure protection. Our recommendations seek to provide structures for the partnership needed to assure our future security. Further, they seek to define new ways for approaching infrastructure assurance—ways that recognize the new thinking required in the Information Age, the new international security environment emerging from our victory in the Cold War and both the promise and danger of technology moving at breakneck speed.

We do not so much offer solutions as directions—compass headings that will help navigate through a new geography and ensure the continuity of the infrastructures that underpin America's economic, military, and social strength.